UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

LARRY SIEGAL, STEVEN CHOJNICKI, and KEVIN DOWD, individually and on behalf of all others similarly situated, Plaintiffs, v. **MR. COOPER GROUP INC.**, Defendant.	Case No. 3:23-cv-02485 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Larry Siegal, Steven Chojnicki, and Kevin Dowd ("Plaintiffs") bring this Class Action Petition ("Petition") against Mr. Cooper Group Inc. ("Mr. Cooper" or "Defendant"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Petition against Mr. Cooper for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, upon information and belief, names, Social Security numbers, addresses, phone numbers, dates of birth, zip code, and states of residence—information used by Mr. Cooper for its business operations (collectively, "personally identifiable information" or "PII").

2. Defendant is the 3rd largest mortgage and loan servicer in the country, providing

services to "4.3 million customers nationwide[.]"[1]

3. Upon information and belief, former and current Mr. Cooper customers are required to entrust Defendant with an extensive amount of their PII, used for Defendant's business, in order to obtain mortgage or loan services at Mr. Cooper. Defendant retains this information for at least many years and even after the relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On October 31, 2023, Defendant "became the target of a cybersecurity incident[.]"[2]

6. Defendant failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

7. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and

[1] https://www.mrcooper.com/about-us/overview (last visited Nov. 7, 2023).
[2] The "Notice Letter". A sample copy is available at https://incident.mrcooperinfo.com/ (last visited Nov. 7, 2023).

effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence, at a minimum, and violates federal and state statutes.

8. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

9. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

10. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to damages and injunctive and other equitable relief.

PARTIES

11. Plaintiff Larry Siegal is a natural person, resident, and a citizen of Skokie, Illinois. Defendant obtained and continues to maintain Plaintiff Siegal's PII, and Defendant owed him a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Siegal would not have entrusted his PII to Defendant had he known that Defendant failed to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

12. Plaintiff Steven Chojnicki is a natural person, resident, and a citizen of Sturbridge, Massachusetts. Defendant obtained and continues to maintain Plaintiff Chojnicki's PII, and Defendant owed him a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Chojnicki would not have entrusted his PII to Defendant had he known that Defendant failed to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

13. Plaintiff Kevin Dowd is a natural person, resident, and a citizen of De Soto, Missouri. Defendant obtained and continues to maintain Plaintiff Dowd's PII, and Defendant owed him a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Dowd would not have entrusted his PII to Defendant had he known that Defendant failed to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

14. Defendant Mr. Cooper Group Inc. is a corporation organized under the state laws of Delaware with its principal place of business located at 8590 Cypress Waters Boulevard, Coppell, Texas 75019. The registered agent for service of process is Corporation Service Company dba CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620,

Austin, TX 78701-3218.

JURISDICTION AND VENUE

15. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, including Plaintiffs, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

16. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in the Dallas Division of the Northern District of Texas, regularly conducts business in Texas, and has sufficient minimum contacts in Texas.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in the Dallas Division of the Northern District of Texas and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District

FACTUAL ALLEGATIONS

Defendant's Business

18. Defendant is the 3rd largest mortgage and loan servicer in the country, providing services to "4.3 million customers nationwide[.]"[3]

19. Plaintiffs and Class Members are or were customers of Mr. Cooper.

20. In order to obtain mortgage or loan services at Mr. Cooper, Plaintiffs and Class Members were required to provide sensitive and confidential PII to Defendant.

21. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiffs and Class Members, that the PII collected from them as a

[3] https://www.mrcooper.com/about-us/overview (last visited Nov. 7, 2023).

condition of obtaining mortgage or loan services at Mr. Cooper would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

22. Indeed, the Defendant's Privacy Policy provides that: "[k]eeping financial information is one of our most important responsibilities. Only those persons who need it to perform their job responsibilities are authorized to access your information. We take commercially reasonable precautions to protect your information and limit disclosure by maintaining physical, electronic and procedural safeguards."[4]

23. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

24. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

25. Defendant had obligations created by FTC Act, Gramm-Leach Bliley Act, contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

26. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach

[4] https://www.mrcooper.com/privacy (last visited Nov. 7, 2023).

27. On or about November 2, 2023, Defendant began sending Plaintiffs and other victims of the Data Breach a Notice of Cyber Security Incident email (the "Notice Letter") informing them that:

> On October 31st, Mr. Cooper became the target of a cyber security incident and took immediate steps to lock down our systems in order to keep your data safe. We are working to resolve the issue as quickly as possible.
>
> . . .
>
> For updated information, we encourage you to visit https://incident.mrcooperinfo.com/.[5]

28. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

29. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiffs and Class Members, including, upon information and belief, their Social Security numbers and other sensitive information. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

30. Plaintiffs further believes that their PII and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members,

[5] The Notice Letter.

causing the exposure of PII , such as encrypting the information or deleting it when it is no longer needed.

32. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[6]

33. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[7] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

34. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[8] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[9] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[10] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data

---

[6] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Oct. 17, 2022).

[7] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[8] *2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report*

[9] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs

[10] *Id.*

are destroyed.[11]

35. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

[11] *Id.*

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[12]

36. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential full compromise;
> - Include IT Pros in security discussions
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**
>
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events;

[12] *Id.* at 3–4.

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[13]

37. Given that Defendant was storing the PII of its current and former customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

38. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of, upon information and belief, hundreds of thousands of individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' PII

39. As a condition to obtain mortgage or loan services at Mr. Cooper, Plaintiffs and Class Members are required to give their sensitive and confidential PII to Defendant. Defendant retains this information even after the relationship has ended and Defendant is no longer required to retain this information.

40. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

41. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained

[13] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Oct. 17, 2022).

securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

42. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members.

43. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk because Loan Service Providers in Possession of PII are Particularly Susceptible to Cyber Attacks

44. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII, like Defendant, preceding the date of the breach.

45. Data breaches, including those perpetrated against loan service providers that store PII in their systems, have become widespread.

46. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[14]

47. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

[14] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

48. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[15]

49. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

50. Defendant knew and understood that unprotected or exposed PII in the custody of educational institutions, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

51. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

52. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII .

53. Defendant was, or should have been, fully aware of the unique type and the

[15] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

54. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

55. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

56. As a loan service provider in custody of its customers' PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

57. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[16] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[17]

58. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[18]

59. For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

60. Social Security numbers, which, upon information and belief, were compromised for some of the Class Members as alleged herein, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[21]

---

[17] *Id.*
[18] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).
[19] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[20] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[21] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

61. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

64. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[23]

65. Among other forms of fraud, identity thieves may obtain driver's licenses,

---

[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 17, 2022).

[23] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

government benefits, medical services, and housing or even give false information to police.

66. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

Defendant Fails to Comply with FTC Guidelines

67. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

68. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[25]

---

[24] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

[25] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

69. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[26]

70. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. These FTC enforcement actions include actions against loan service providers, like Defendant.

73. Defendant failed to properly implement basic data security practices.

74. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

75. Upon information and belief, Defendant was at all times fully aware of its

[26] *Id.*

obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with the Gramm-Leach-Bliley Act

76. Mr. Cooper is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

77. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

78. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

79. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

80. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

81. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and

conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

82. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendant's network systems.

83. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified

through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

84. As alleged herein, Defendant violated the Safeguard Rule.

85. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

86. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class Members with a non-affiliated third party without providing Plaintiffs and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendant Fails to Comply with Industry Standards

87. As noted above, experts studying cyber security routinely entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

88. Several best practices have been identified that a minimum should be implemented by loan service providers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-

factor authentication.

89. Other best cybersecurity practices that are standard in the loan servicing industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

90. Upon information and belief Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

91. These foregoing frameworks are existing and applicable industry standards in the loan servicing industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

92. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Plaintiffs' and Class Member's Risk of Identity Theft

93. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

94. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

95. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

96. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

97. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a

victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

98. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[27]

99. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

100. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers

[27] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

101. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class Members.

102. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

103. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

104. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

105. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

106. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, contacting credit bureaus to ensure their accounts

are secure, reporting the Data Breach to the proper authorities, monitoring their credit card statement for any signs of fraudulent activity, which may take years to detect.

107. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

108. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

109. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[29]

Diminution of Value of PII

110. PII is a valuable property right.[30] Its value is axiomatic, considering the value of

---

[28] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[29] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

[30] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching

Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

111. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[31]

112. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[32]

113. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[33,34] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[35]

114. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

115. Based on the foregoing, the information compromised in the Data Breach is

---

a level comparable to the value of traditional financial assets.") (citations omitted).

[31] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

[32] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[33] https://datacoup.com/

[34] https://digi.me/what-is-digime/

[35] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, *e.g.,* Social Security numbers and names.

116. The fraudulent activity resulting from the Data Breach may not come to light for years.

117. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

118. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

119. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

120. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable & Necessary

121. Given the type of targeted attack in this case, the sophisticated criminal activity,

and the type of PII involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

122. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

123. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[36] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

124. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

125. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

[36] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

126. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant for mortgage or loan services under certain terms, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for services and data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCES

Plaintiff Larry Siegal

127. Plaintiff Siegal is a current Mr. Cooper customer.

128. In order to obtain mortgage or loan services at Mr. Cooper, he was required to provide his PII, directly or indirectly, to Defendant, including his name, date of birth, Social Security number, and other sensitive information.

129. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's PII in its system.

130. Plaintiff Siegal is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Siegal would not have provided his PII to Defendant had he known that Defendant would fail to reasonably safeguard that data from unauthorized access.

131. Plaintiff Siegal received the Notice Letter, by email, directly from Defendant, on or about November 7, 2023. Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including, upon information and belief, his full name, Social Security

number, address, phone number, date of birth, zip code, and stats of residence.

132. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter as well as monitoring his credit card statement for any signs of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

133. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

134. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

135. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

136. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

137. Plaintiff Siegal has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Steven Chojnicki

138. Plaintiff Chojnicki is a current Mr. Cooper customer.

139. In order to obtain mortgage or loan services at Mr. Cooper, he was required to provide his PII to Defendant, including his name, date of birth, Social Security number, and other sensitive information.

140. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's PII in its system.

141. Plaintiff Chojnicki is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Chojnicki would not have provided his PII to Defendant had he known that Defendant would fail to reasonably safeguard that data from unauthorized access.

142. Plaintiff Chojnicki received the Notice Letter, by email, directly from Defendant, on or about November 7, 2023. Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including, upon information and belief, his full name, Social Security number, address, phone number, date of birth, zip code, and stats of residence.

143. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy

of the Data Breach upon receiving the Notice Letter, contacting credit bureaus to ensure his accounts are secure, reporting the Data Breach to the FTC and Massachusetts Attorney General, and monitoring his credit card statement for any signs of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

144. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

145. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

146. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

147. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

148. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

149. Plaintiff Chojnicki has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Kevin Dowd

150. Plaintiff Dowd is a current Mr. Cooper customer.

151. In order to obtain mortgage or loan services at Mr. Cooper, he was required to provide his PII to Defendant, including his name, date of birth, Social Security number, and other sensitive information.

152. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's PII in its system.

153. Plaintiff Dowd is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Dowd would not have provided his PII to Defendant had he known that Defendant would fail to reasonably safeguard that data from unauthorized access.

154. Plaintiff Dowd received the Notice Letter, by email, directly from Defendant, on or about November 7, 2023. Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including, upon information and belief, his full name, Social Security number, address, phone number, date of birth, zip code, and stats of residence.

155. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy

of the Data Breach upon receiving the Notice Letter as well as monitoring his financial accounts for any signs of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

156. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

157. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

158. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

159. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

160. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be

at increased risk of identity theft and fraud for years to come.

161. Plaintiff Dowd has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

162. Plaintiffs bring this action on behalf of themselves and all other persons similarly situated.

163. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All persons in the United States whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in November 2023 (the "Class").
>
> **Illinois Subclass**
> All persons in the state of Illinois whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in November 2023 (the "Illinois Subclass").

164. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

165. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

166. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Although the precise number of individuals impacted in the Data

Breach is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, hundreds of thousands of persons were impacted in the Data Breach. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

167. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant was unjustly enriched;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

l. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

168. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class member, was compromised in the Data Breach.

169. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

170. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

171. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law

and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

172. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

173. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

174. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST COUNT
Negligence
(On Behalf of Plaintiffs and the Class)

175. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

176. Defendant requires its customers, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of providing its mortgage and loan services.

177. Defendant gathered and stored the PII of Plaintiffs and Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

178. Plaintiffs and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

179. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

180. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

181. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

182. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

183. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

184. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary part of being customers of Defendant.

185. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

186. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

187. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

188. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

189. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

190. Defendant breached its duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk

computers, even after discovery of the data breach.

191. Defendant violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

192. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

193. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes negligence.

194. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

195. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

196. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the loan servicing industry.

197. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

198. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

199. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

200. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

201. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

202. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

203. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

204. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

205. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed

as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

206. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

207. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

208. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

209. Plaintiffs and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

210. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

211. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

212. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

213. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

214. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

215. Defendant violated Section 5 of the FTC Act, GLBA, and similar state statutes by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on

Defendant's systems.

216. Defendant's violation of Section 5 of the FTC Act, GLBA, and similar state statutes constitutes negligence *per se.*

217. Class members are consumers within the class of persons Section 5 of the FTC Act, GLBA, and similar state statutes were intended to protect.

218. Moreover, the harm that has occurred is the type of harm the FTC Act, GLBA, and similar state statutes were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

219. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

220. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

221. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

222. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

223. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

224. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

225. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

226. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

THIRD COUNT
Breach Of Implied Contract
(On Behalf of Plaintiffs and the Class)

227. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

228. When Plaintiffs and Class Members provided their PII to Defendant in exchange for obtaining mortgage or loan services at Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any PII that it was no longer required to maintain.

229. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

230. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

231. In accepting the PII of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

232. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including the FTC Act, and were consistent with industry standards.

233. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

234. Plaintiffs and Class Members would not have entrusted their PII to Defendant in

the absence of the implied contract between them and Defendant to keep their information reasonably secure.

235. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

236. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

237. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII or to destroy it once it was no longer necessary to retain the PII.

238. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

239. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

240. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

241. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

242. This count is pleaded in the alternative to the Breach of Implied Contract claim

(Count III) above.

243. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by Plaintiffs and Class Members.

244. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

245. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their PII and paid money to Defendant in connection with obtaining mortgage or loan services at Defendant and/or its agents, and in so doing, provided Defendant with their PII based on the understanding that the benefits derived therefrom would, in part, be used to fund adequate data security. In exchange, Plaintiffs and Class Members should have received from Defendant the mortgage or loan services that were the subject of the transaction and have their PII protected with adequate data security.

246. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

247. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and instead directed those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

248. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

249. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

250. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

251. Defendant obtained a benefit from Plaintiffs and Class Members by fraud and/or the taking of an undue advantage, in that it misrepresented and omitted material information concerning its data security practices when Plaintiffs and Class Members relied upon it to safeguard their PII against foreseeable risks.

252. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

253. Plaintiffs and Class Members have no adequate remedy at law.

254. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

255. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class

Members have suffered and will continue to suffer other forms of injuries and/or harms.

256. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

FIFTH COUNT
Violation Of The Illinois Consumer Fraud Act
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On Behalf of Plaintiff Siegal and the Illinois Subclass)

257. Plaintiff Siegal ("Plaintiff" for the purposes of this count) re-alleges and incorporates the above allegations as if fully set forth herein, and brings this claim on behalf of himself and the Illinois Subclass (the "Class" for the purposes of this count).

258. Plaintiff and the Class are "consumers" as that term is defined in 815 ILL. COMP. STAT. § 505/1(e).

259. Plaintiff, the Class, and Defendant are "persons" as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

260. Defendant is engaged in "trade" or "commerce," including the provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

261. Defendant engages in the "sale" of "merchandise" (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

262. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering for sale, and selling loan and mortgage services in the State of Illinois.

263. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale

and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including, but not limited to, the following:

a. failure to maintain adequate computer systems and data security practices to safeguard current and former customers' PII;

b. failure to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the personal information it was collecting and maintaining from theft;

c. failure to disclose in a timely and accurate manner to Plaintiff and the Class Members the material fact of Defendant's data breach;

d. misrepresenting material facts to Plaintiff and the Class, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft;

e. misrepresenting material facts to the class, in connection with the sale of goods and services, by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class members' PII, and

f. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Class members' PII from further unauthorized disclosure, release, data breaches, and theft.

264. In addition, Defendant's failure to disclose that its computer systems were not well protected and that Plaintiff's and Class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices

because Defendant knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Class; and (b) defeat Plaintiff's and Class members' ordinary, foreseeable and reasonable expectations concerning the security of their PII on Defendant's servers.

265. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Defendant's offering of goods and services and storing Plaintiff's and Class members' PII on its servers, in violation of the Illinois CFA.

266. Defendant also engaged in unfair acts and practices by failing to maintain the privacy and security of class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach.

267. These unfair acts and practices violated duties imposed by laws including Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

268. Defendant's wrongful practices occurred in the course of trade or commerce.

269. Defendant's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendant that applied to all Class members and were repeated continuously before and after Defendant obtained PII from Plaintiff and Class members.

270. All Class members have been adversely affected by Defendant conduct and the public was and is at risk as a result thereof.

271. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered harm, including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of

the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

272. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiff seeks actual, compensatory, and punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the Illinois CFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class and Illinois Subclass;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

1. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
2. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
3. Requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
4. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
5. Prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;
6. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to

promptly correct any problems or issues detected by such third-party security auditors;

7. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

8. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

9. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

10. Requiring Defendant to conduct regular database scanning and securing checks;

11. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

12. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

13. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

14. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

15. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

16. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

17. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: November 8, 2023

Respectfully submitted,

s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
214-744-3000
214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Attorney For Plaintiffs

**Pro Hac Vice* application forthcoming